



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,474	12/14/2001	Barbir Abdulkader	08889801US	1008

26123 7590 05/02/2005

BORDEN LADNER GERVAIS LLP
WORLD EXCHANGE PLAZA
100 QUEEN STREET SUITE 1100
OTTAWA, ON K1P 1J9
CANADA

EXAMINER

CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 05/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/014,474

Applicant(s)

ABDULKADER, BARBIR

Examiner

David G. Cervetti

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 December 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 December 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☒ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 6/7/02.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 101, 130, 185, 199 (figure 1). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

2. The abstract of the disclosure is objected to because it exceeds 150 words in length. Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that

Art Unit: 2136

the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

3. The disclosure is objected to because of the following informalities: "and the receiver 180, 185" (page 6, line 12), perhaps "170, 180" was intended. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claim 1-9 is rejected under 35 U.S.C. 102(a) as being anticipated by Wright (US Patent Number: 6,052,466).

Regarding claim 1, Wright teaches a packet-based encryption system comprising: a transmitting device to encrypt data and to insert a pseudo-random key in a transmitted packet (figure 3, Party A, column 5, lines 58-67, column 6, lines 1-21, figure 5, column 6, lines 46-67); and a receiving device to receive and to decrypt said data in said transmitted packet using said pseudo-random key (figure 3, Party B, column 5, lines 58-67, column 6, lines 1-21, figure 5, column 6, lines 46-67).

Regarding claim 2, Wright teaches wherein said transmitting device further comprises: means to generate a random number (column 5, lines 24-27); a first one-way cryptographic hash function means to generate a hashed number from said random number (column 5, lines 27-29, column 2, lines 20-25); a first streaming cipher algorithm using a seed to encrypt said hashed number (column 6, lines 22-45); encryption means to encrypt said data using results of said first streaming cipher algorithm (column 6, lines 22-45); and means to insert said random number in a specified field of said transmitted packet (figure 5, column 6, lines 46-67).

Regarding claim 3, Wright teaches wherein said receiving device further comprises: means to remove said random number from said specified field of said transmitted packet (column 6, lines 22-45); a second one-way cryptographic hash function means to generate a second hashed number from said random number (column 5, lines 43-57); a second streaming cipher algorithm using a seed to encrypt said second hashed number (column 6, lines 22-45); and decryption means to decrypt said data using results of said second streaming cipher algorithm (column 6, lines 22-45).

Regarding claim 4, Wright teaches wherein said first one-way cryptographic hash function and said second one-way cryptographic hash function use the same algorithm and use a same first seed or key (column 5, lines 20-25, 58-67, column 11, lines 8-21).

Regarding claim 5, Wright teaches wherein said first streaming cipher algorithm and said second streaming cipher algorithm are the same and use a same second seed or key (column 5, lines 58-67, column 6, lines 1-21).

Regarding claim 6, Wright teaches wherein said encryption means and said decryption means use the same third key and algorithm (column 5, lines 58-67, column 6, lines 1-21).

Regarding claim 7, Wright teaches wherein said transmitting device further comprises: means to generate a random number (column 5, lines 24-27); a first one-way cryptographic hash function means to generate a hashed number from said random number (column 5, lines 27-29, column 2, lines 20-25); a third one-way cryptographic hash function using a seed to encrypt said hashed number (column 6,

Art Unit: 2136

lines 22-45, column 11, lines 8-21); encryption means to encrypt said data using results of said third one-way cryptographic hash function (column 6, lines 22-45, column 11, lines 8-21); and means to insert said random number in a specified field of said transmitted packet (figure 5, column 6, lines 46-67).

Regarding claim 8, Wright teaches wherein said receiving device further comprises: means to remove said random number from said specified field of said transmitted packet (column 6, lines 22-45); a second one-way cryptographic hash function means to generate a second hashed number from said random number (column 5, lines 43-57); a fourth one-way cryptographic hash function using a seed to encrypt said second hashed number (column 6, lines 22-45, column 11, lines 8-21); and decryption means to decrypt said data using results of said fourth one-way cryptographic hash function (column 6, lines 22-45).

Regarding claim 9, Wright teaches wherein said third one-way cryptographic hash function and said fourth one-way cryptographic hash function are the same and use a same fourth seed or key (column 5, lines 20-25, 58-67, column 11, lines 8-21).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wright.

Regarding claim 10, Wright teaches encrypting data and inserting a pseudo-random key in a transmitted packet with said encrypted data (column 5, lines 58-67, column 6, lines 1-21, figure 5, column 6, lines 46-67); and decrypting said data in said transmitted packet with said inserted pseudo-random key (column 5, lines 58-67, column 6, lines 1-21, figure 5, column 6, lines 46-67). Wright does not expressly disclose using a symmetric key-based stream cipher, but suggests that rearrangements, modifications, and substitutions (column 11, lines 8-21). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a symmetric key-based stream cipher instead of public key cryptography in the method of Wright. One of ordinary skill in the art would have been motivated to do so because it was well known in the art that symmetric key cryptography was more efficient (faster) than public key cryptography, while public key cryptography offers more security (more difficult to decrypt).

Regarding claim 11, Wright teaches at the transmitting end: generating a random number (column 5, lines 24-27); generating a hashed number from said random number

using a first one-way cryptographic hash function (column 5, lines 27-29, column 2, lines 20-25); providing a first streaming cipher algorithm using said hashed number as a seed (column 6, lines 22-45); encrypting said data using results of said first streaming cipher algorithm (column 6, lines 22-45); and inserting said random number in a specified field of said transmitted packet (figure 5, column 6, lines 46-67); at the receiving end: removing said random number from said specified field of said transmitted packet (column 6, lines 22-45); generating a second hashed number from said random number using a second one-way cryptographic hash function (column 5, lines 43-57); providing a second streaming cipher algorithm using said hashed number as a seed (column 6, lines 22-45); and decrypting said data using results of said second streaming cipher algorithm using said second hashed number as a seed (column 6, lines 22-45).

Regarding claim 12, Wright teaches at the transmitting end: generating a random number (column 5, lines 24-27); generating a hashed number from said random number using a first one-way cryptographic hash function (column 5, lines 27-29, column 2, lines 20-25); providing a third one-way cryptographic hash function using a seed to encrypt said hashed number (column 6, lines 22-45, column 11, lines 8-21); encrypting said data using results of said first streaming cipher algorithm (column 6, lines 22-45); and inserting said random number in a specified field of said transmitted packet (figure 5, column 6, lines 46-67); at the receiving end: removing said random number from said specified field of said transmitted packet (column 6, lines 22-45); generating a second hashed number from said random number using a second one-way cryptographic hash

Art Unit: 2136

function (column 5, lines 43-57); providing a fourth one-way cryptographic hash function using a seed to encrypt said second hashed number (column 6, lines 22-45, column 11, lines 8-21); and decrypting said data using results of said second streaming cipher algorithm using said second hashed number as a seed (column 6, lines 22-45).


Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, Off on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100